IN THE CLAIMS:

Claims 1, 2, and 33 are amended. No claims are cancelled or added. All pending claims and their present status are produced below.

1. (Currently amended) A method for providing a unique identification of monitored network data instances flowing across various connections between networked devices, the unique identification being derived from information contained entirely within each instance of the network data, the method comprising:

using at least one monitoring device to monitor a network data instance flowing across at least one data connection;

deriving from the data instance certain information which collectively provides a unique identification of the network data instance;

assembling the derived information into an input string for a hash function; and

using the output string of the hash function as a signature which represents a unique ~~identifer~~ identifier of the network data instance.

2. (Currently amended) The method according to Claim 1, wherein the deriving step includes:

deriving from the data instance a source and destination address for the data;

deriving from the data instance a source and destination port associated with the networked devices;

deriving from the data instance at least one sequence number associated with data instance[;].

3. (Original) The method according to Claim 1, which further includes:

attaching the signature to at least one data report associated with the network data instance; and

transmitting the data reports and signatures from each monitoring device to a central collecting device.

4. (Original) The method according to Claim 3, wherein a timestamp is further associated with each data report before it is transmitted to the central collector.

5. (Original) The method according to Claim 3, wherein the central collecting device uses the signatures to eliminate duplicate data reports that might come in from different monitoring devices positioned at different locations on the network.

6. (Original) The method according to Claim 1, wherein network data instances are data packets as part of a TCP/IP (Transmission Control Protocol/Internet Protocol) client-server network.

7. (Original) The method according to Claim 6, wherein the source and destination addresses include a client IP address and a server IP address.

8. (Original) The method according to Claim 7, wherein the source and destination port include a client port number and a server port number.

9. (Previously Presented) The method according to Claim 2, wherein the at least one sequence number includes a client sequence number or a server sequence number.

10. (Original) The method according to Claim 9, wherein the at least one sequence number includes both a client sequence number and a server sequence number.

11. (Original) The method according to Claim 2, wherein the input string information does not include sequence numbers.

12. (Original) The method according to Claim 11, wherein the network data instances are datagrams as part of a UDP/IP (User Datagram Protocol/Internet Protocol) network.

13. (Original) The method according to Claim 1, which further includes: truncating the signature to include fewer bits than the hash function output string.

14. (Original) The method according to Claim 1, which further includes: adding flag bits to the signature which indicate the type of application associated with the network data instance.

15. (Original) The method according to Claim 3, wherein the monitor serves as a data reduction device for data report and signature information being sent to the central data collector.

16. (Original) The method according to Claim 1, wherein the monitoring device operates to directly monitor the network data.

17. (Original) The method according to Claim 1, wherein the monitoring device operates to indirectly monitor the network data.

18. (Original) An apparatus for providing a unique identification of monitored network data instances flowing across various connections between networked devices, the unique identification being derived from information contained entirely within each instance of the network data, the apparatus comprising:

at least one monitoring device positioned to monitor a network data instance flowing across at least one data connection;

a hash function device having an input string and an output string, the input string assembled from certain information derived from the network data instance,

the information collectively providing a unique identification of the network data instance;

wherein the output string is used as a signature which represents a unique identifier of the network data instance.

19. (Original) The apparatus according to Claim 18, wherein information derived from the network data instance includes at least:

a source and destination address derived from the network data instance;

a source and destination port associated with the networked devices; and

at least one sequence number associated with network data instance.

20. (Original) The apparatus according to Claim 18, which further includes:

at least one data report associated with the network data instance, the signature being attached to the data report; and

a central collection device that receives transmitted data reports and signatures from each monitoring device.

21. (Original) The apparatus according to Claim 20, wherein a timestamp is further associated with each data report before it is transmitted to the central collector.

22. (Original) The apparatus according to Claim 20, wherein the central collecting device uses the signatures to eliminate duplicate data reports that might come in from different monitoring devices positioned at different locations on the network.

23. (Previously presented) The apparatus according to Claim 19, wherein network data instances are data packets as part of a TCP/IP (Transmission Control Protocol/Internet Protocol) client-server network.

24. (Original) The apparatus according to Claim 23, wherein the source and destination addresses include a client IP address and a server IP address.

25. (Original) The apparatus according to Claim 24, wherein the source and destination port include a client port number and a server port number.

26. (Original) The apparatus according to Claim 25, wherein the at least one sequence number includes a client sequence number or a server sequence number.

27. (Original) The apparatus according to Claim 26, wherein the at least one sequence number also includes both a client sequence number and a server sequence number.

28. (Original) The apparatus according to Claim 19, wherein the input string information does not include sequence numbers.

29. (Original) The apparatus according to Claim 28, wherein the network data instances are datagrams as part of a UDP/IP (User Datagram Protocol/Internet Protocol) network.

30. (Original) The method according to Claim 18, wherein the signature is truncated to include fewer bits than the hash function output string.

31. (Original) The method according to Claim 18, wherein flag bits are added to the signature which indicate the type of application associated with the network data instance.

32. (Original) The method according to Claim 20, wherein the monitor serves as a data reduction device for data report and signature information being sent to the central data collector.

33. (Currently amended) A method for providing a unique signature of monitored network data packets flowing across various connections between networked devices,

the unique signature being derived from information contained entirely within each instance of the network data packet, the method comprising:

using at least one monitoring device to monitor a network data packet flowing across at least one data connection;

deriving from the data packet a source and destination address for the data;

deriving from the data packet a source and destination port associated with the networked devices;

deriving from the data packet at least one sequence number associated with data instance;

assembling the derived addresses, ports, and at least one sequence number information into an input string for a hash function; ~~and~~

using the output string of the hash function as the signature which represents a unique ~~identifer~~ identifier of the network data packet[.];

attaching the signature to at least one data report associated with the network data packet; and

transmitting the data reports and signatures from each monitoring device to a central collecting device for analysis.